Listing of Claims:

1. (Currently Amended) A method of improving security processing in a computing network, comprising:

providing security processing in an operating system kernel;

providing an application program which makes use of the operating system kernel during execution;

providing security policy information that is usable for more than one executing application program;

executing the application program; and

selectably encrypting at least one communication of the executing application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information.

2. (Original) The method according to claim 1, wherein the security policy information is stored in a security repository.

3. (Cancelled)

4. (Previously Presented) The method according to claim 1, wherein the conditions comprise network addresses.

5. (Currently Amended) The method according to claim 4, wherein the network addresses specify at least one ~~or more~~ of server addresses and destination addresses.

6. (Currently Amended) The method according to claim 4, wherein the network addresses comprise at least one of ranges of source addresses and ~~and/or~~ ranges of destination addresses.

7. (Currently Amended) The method according to claim 1, wherein the conditions comprise at least one of ~~or more~~ port numbers and ~~and/or one or more~~ port number ranges.

8. (Currently Amended) The method according to claim 1, wherein the conditions comprise at least one ~~or more~~ job name ~~names~~.

9. (Currently Amended) The method according to claim 1, wherein the conditions comprise at least one ~~or more~~ client identifier ~~identifiers~~.

10. (Currently Amended) The method according to claim 1, further comprising checking the security policy information when the executing application program establishes a connection, and wherein the communications on that connection are encrypted ~~according to a result of the checking step~~.

11. (Currently Amended) The method according to claim 1, ~~whereby~~ wherein communications from the executing application program ~~may be~~ are encrypted even though the provided application program has no code for security processing.

12. (Currently Amended) The method according to claim 1, wherein the provided application program invokes at least one ~~or more~~ security directive ~~directives~~, and further comprising executing, during execution of the provided application program, at least one ~~or more~~ of the invoked security directives.

13. (Previously Presented) The method according to claim 1, wherein, when a result of evaluating the security policy information so indicates, communications on only some sockets of a port are encrypted.

14. (Original) The method according to claim 1, wherein the provided security processing operates in a Transmission Control Protocol layer of the operating system kernel.

15. (Original) The method according to claim 1, wherein the provided security processing implements Secure Sockets Layer.

16. (Previously Presented) The method according to claim 1, wherein the provided security processing implements Transport Layer Security.

17. (Currently Amended) A system for improving security processing in a computing network, comprising:

means for performing security processing in an operating system kernel;

security policy information that is usable for more than one executing application program specifying at least one condition ~~or more conditions~~ under which the means for performing security processing is to be activated;

means for executing an application program which makes use of the operating system kernel during execution; and

means for selectably encrypting, according to the conditions specified by the security policy information, at least one communication of the executing application program using the means for performing security processing.

18. (Currently Amended) A computer program product for improving security processing in a computing network, the computer program product comprising:

a computer usable medium having computer readable program code embodied ~~thereintherewith~~ therein, the computer usable medium comprising:

computer-readable program code configured to perform security processing in an operating system kernel;

computer-readable program code configured to access security policy information that is usable for more than one executing application program, the security policy information specifying at least one condition ~~or more conditions~~ under which the computer-readable program code configured to perform security processing is to be activated;

computer-readable program code configured to execute an application program which makes use of the operating system kernel during execution; and

computer-readable program code configured to selectably encrypt, according to the conditions specified by the security policy information, at least one communication of the executing application program using the computer-readable program code configured to perform security processing.